



Configuring Control Plane Policing

This chapter contains the following sections:

- [Finding Feature Information, on page 1](#)
- [Information About CoPP, on page 1](#)
- [Guidelines and Limitations for CoPP, on page 19](#)
- [Default Settings for CoPP, on page 22](#)
- [Configuring CoPP, on page 22](#)
- [Verifying the CoPP Configuration, on page 32](#)
- [Displaying the CoPP Configuration Status, on page 34](#)
- [Monitoring CoPP, on page 34](#)
- [Monitoring CoPP with SNMP, on page 38](#)
- [Clearing the CoPP Statistics, on page 38](#)
- [Configuration Examples for CoPP, on page 39](#)
- [Changing or Reapplying the Default CoPP Policy Using the Setup Utility, on page 42](#)
- [Additional References for CoPP, on page 43](#)
- [Feature History for CoPP, on page 44](#)

Finding Feature Information

Your software release might not support all the features documented in this module. For the latest caveats and feature information, see the Bug Search Tool at <https://tools.cisco.com/bugsearch/> and the release notes for your software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the "New and Changed Information" chapter or the Feature History table in this chapter.

Information About CoPP

Control Plane Policing (CoPP) protects the control plane and separates it from the data plane, which ensures network stability, reachability, and packet delivery.

This feature allows a policy map to be applied to the control plane. This policy map looks like a normal QoS policy and is applied to all traffic destined to any of the IP addresses of the router or Layer 3 switch. A common attack vector for network devices is the denial-of-service (DoS) attack, where excessive traffic is directed at the device interfaces.

The Cisco NX-OS device provides CoPP to prevent DoS attacks from impacting performance. Such attacks, which can be perpetrated either inadvertently or maliciously, typically involve high rates of traffic destined to the supervisor module or CPU itself.

The supervisor module divides the traffic that it manages into three functional components or planes:

Data plane

Handles all the data traffic. The basic functionality of a Cisco NX-OS device is to forward packets from one interface to another. The packets that are not meant for the switch itself are called the transit packets. These packets are handled by the data plane.

Control plane

Handles all routing protocol control traffic. These protocols, such as the Border Gateway Protocol (BGP) and the Open Shortest Path First (OSPF) Protocol, send control packets between devices. These packets are destined to router addresses and are called control plane packets.

Management plane

Runs the components meant for Cisco NX-OS device management purposes such as the command-line interface (CLI) and Simple Network Management Protocol (SNMP).

The supervisor module has both the management plane and control plane and is critical to the operation of the network. Any disruption or attacks to the supervisor module will result in serious network outages. For example, excessive traffic to the supervisor module could overload and slow down the performance of the entire Cisco NX-OS device. Another example is a DoS attack on the supervisor module that could generate IP traffic streams to the control plane at a very high rate, forcing the control plane to spend a large amount of time in handling these packets and preventing the control plane from processing genuine traffic.

Examples of DoS attacks are as follows:

- Internet Control Message Protocol (ICMP) echo requests
- IP fragments
- TCP SYN flooding

These attacks can impact the device performance and have the following negative effects:

- Reduced service quality (such as poor voice, video, or critical applications traffic)
- High route processor or switch processor CPU utilization
- Route flaps due to loss of routing protocol updates or keepalives
- Unstable Layer 2 topology
- Slow or unresponsive interactive sessions with the CLI
- Processor resource exhaustion, such as the memory and buffers
- Indiscriminate drops of incoming packets

**Caution**

It is important to ensure that you protect the supervisor module from accidental or malicious attacks by configuring control plane protection.

Control Plane Protection

To protect the control plane, the Cisco NX-OS device segregates different packets destined for the control plane into different classes. Once these classes are identified, the Cisco NX-OS device polices the packets, which ensures that the supervisor module is not overwhelmed.

Control Plane Packet Types

Different types of packets can reach the control plane:

Receive packets

Packets that have the destination address of a router. The destination address can be a Layer 2 address (such as a router MAC address) or a Layer 3 address (such as the IP address of a router interface). These packets include router updates and keepalive messages. Multicast packets can also be in this category where packets are sent to multicast addresses that are used by a router.

Exception packets

Packets that need special handling by the supervisor module. For example, if a destination address is not present in the Forwarding Information Base (FIB) and results in a miss, the supervisor module sends an ICMP unreachable packet back to the sender. Another example is a packet with IP options set.

Redirected packets

Packets that are redirected to the supervisor module. Features such as Dynamic Host Configuration Protocol (DHCP) snooping or dynamic Address Resolution Protocol (ARP) inspection redirect some packets to the supervisor module.

Glean packets

If a Layer 2 MAC address for a destination IP address is not present in the FIB, the supervisor module receives the packet and sends an ARP request to the host.

All of these different packets could be maliciously used to attack the control plane and overwhelm the Cisco NX-OS device. CoPP classifies these packets to different classes and provides a mechanism to individually control the rate at which the supervisor module receives these packets.

Classification for CoPP

For effective protection, the Cisco NX-OS device classifies the packets that reach the supervisor modules to allow you to apply different rate controlling policies based on the type of the packet. For example, you might want to be less strict with a protocol packet such as Hello messages but more strict with a packet that is sent to the supervisor module because the IP option is set.

Rate Controlling Mechanisms

Once the packets are classified, the Cisco NX-OS device has different mechanisms to control the rate at which packets arrive at the supervisor module. Two mechanisms control the rate of traffic to the supervisor module. One is called policing and the other is called rate limiting.

Using hardware policers, you can define separate actions for traffic that conforms to, exceeds, or violates certain conditions. The actions can transmit the packet, mark down the packet, or drop the packet.

You can configure the following parameters for policing:

Committed information rate (CIR)

Desired bandwidth, specified as a bit rate or a percentage of the link rate.

Peak information rate (PIR)

Desired bandwidth, specified as a bit rate or a percentage of the link rate.

Committed burst (BC)

Size of a traffic burst that can exceed the CIR within a given unit of time and not impact scheduling.

Extended burst (BE)

Size that a traffic burst can reach before all traffic exceeds the PIR.

In addition, you can set separate actions such as transmit or drop for conform, exceed, and violate traffic.

For more information on policing parameters, see the *Cisco Nexus 7000 Series NX-OS Quality of Service Configuration Guide*.

Default Policing Policies

When you bring up your Cisco NX-OS device for the first time, the Cisco NX-OS software installs the default `copp-system-p-policy-strict` policy to protect the supervisor module from DoS attacks. You can set the level of protection by choosing one of the following CoPP policy options from the initial setup utility:

- **Strict**—This policy is 1 rate and 2 color and has a BC value of 250 ms (except for the important class, which has a value of 1000 ms).
- **Moderate**—This policy is 1 rate and 2 color and has a BC value of 310 ms (except for the important class, which has a value of 1250 ms). These values are 25 percent greater than the strict policy.
- **Lenient**—This policy is 1 rate and 2 color and has a BC value of 375 ms (except for the important class, which has a value of 1500 ms). These values are 50 percent greater than the strict policy.
- **Dense**—This policy is 1 rate and 2 color. The classes critical, normal, redirect, exception, undesirable, l2-default, and default have a BC value of 250 ms. The classes important, management, normal-dhcp, normal-dhcp-relay-response, and monitoring have a BC value of 1000 ms. The class l2-unpoliced has a BC value of 5 MB.



Note We recommend this default policy when the chassis is fully loaded with F2 Series modules or loaded with more F2 Series modules than any other I/O modules.

- **Skip**—No control plane policy is applied. In Cisco NX-OS releases prior to 5.2, this option is named none.

If you do not select an option or choose not to execute the setup utility, the Cisco NX-OS software applies strict policing. We recommend that you start with the strict policy and later modify the CoPP policies as required.

The `copp-system-p-policy` policy has optimized values suitable for basic device operations. You must add specific class and access-control list (ACL) rules that meet your DoS protection requirements. The default CoPP policy does not change when you upgrade the Cisco NX-OS software.



Caution Selecting the **skip** option and not subsequently configuring CoPP protection can leave your Cisco NX-OS device vulnerable to DoS attacks.

You can reassign the CoPP default policy by entering the setup utility again using the **setup** command from the CLI prompt or by using the **copp profile** command in Cisco NX-OS Release 5.2 or later releases.

Related Topics

[Changing or Reapplying the Default CoPP Policy](#), on page 30

Default Class Maps

Note The class maps provided here are for Cisco NX-OS Release 6.2(2). Some of the values might vary for previous releases.

The `copp-system-class-exception` class has the following configuration:

```
class-map type control-plane match-any copp-system-p-class-exception
  match exception ip option
  match exception ip icmp unreachable
  match exception ipv6 option
  match exception ipv6 icmp unreachable
```

The `copp-system-class-critical` class has the following configuration:

```
ip access-list copp-system-p-acl-igmp
  permit igmp any 224.0.0.0/3

ip access-list copp-system-p-acl-lisp
  permit udp any any eq 4342

ip access-list copp-system-p-acl-msdp
  permit tcp any gt 1024 any eq 639
  permit tcp any eq 639 any gt 1024

ip access-list copp-system-p-acl-bgp
  permit tcp any gt 1024 any eq bgp
  permit tcp any eq bgp any gt 1024

ip access-list copp-system-p-acl-eigrp
  permit eigrp any any

ip access-list copp-system-p-acl-lisp6
  permit udp any any eq 4342

ip access-list copp-system-p-acl-rip
  permit udp any 224.0.0.0/24 eq rip

ip access-list copp-system-p-acl-ospf
  permit ospf any any

ip access-list copp-system-p-acl-pim
  permit pim any 224.0.0.0/24

  permit udp any any eq 496
  permit ip any 224.0.0.13/32

ipv6 access-list copp-system-p-acl-bgp6
  permit tcp any gt 1024 any eq bgp
  permit tcp any eq bgp any gt 1024

ipv6 access-list copp-system-p-acl-ospf6
  permit 89 any any
```

```

ipv6 access-list copp-system-p-acl-pim6
  permit 103 any FF02::D/128
  permit udp any any eq pim-auto-rp

ipv6 access-list copp-system-p-acl-rip6
  permit udp any ff02::9/64 eq 521

ip access-list copp-system-p-acl-vpc
  permit udp any any eq 3200

ip access-list copp-system-p-acl-mpls-ldp
  permit udp any eq 646 any eq 646
  permit tcp any any eq 646
  permit tcp any eq 646 any

ip access-list copp-system-p-acl-mpls-oam
  permit udp any eq 3503 any

ip access-list copp-system-p-acl-mpls-rsvp
  permit 46 any any

ip access-list copp-system-p-acl-otv-as
  permit udp any any eq 8472

mac access-list copp-system-p-acl-mac-l2pt
  permit any 0100.0ccd.cdd0 0000.0000.0000

mac access-list copp-system-p-acl-mac-otv-isis
  permit any 0100.0cdf.dfdf 0000.0000.0000

mac access-list copp-system-p-acl-mac-fabricpath-isis
  permit any 0180.c200.0041 0000.0000.0000

mac access-list copp-system-p-acl-mac-l3-isis
  permit any 0180.c200.0015 0000.0000.0000
  permit any 0180.c200.0014.0000.0000.0000

class-map type control-plane match-any copp-system-p-class-critical
  match access-group name copp-system-p-acl-bgp
  match access-group name copp-system-p-acl-rip
  match access-group name copp-system-p-acl-vpc
  match access-group name copp-system-p-acl-bgp6
  match access-group name copp-system-p-acl-lisp
  match access-group name copp-system-p-acl-ospf
  match access-group name copp-system-p-acl-rip6
  match access-group name copp-system-p-acl-eigrp
  match access-group name copp-system-p-acl-lisp6
  match access-group name copp-system-p-acl-ospf6
  match access-group name copp-system-p-acl-eigrp6
  match access-group name copp-system-p-acl-otv-as
  match access-group name copp-system-p-acl-mac-l2pt
  match access-group name copp-system-p-acl-mpls-ldp
  match access-group name copp-system-p-acl-mpls-oam
  match access-group name copp-system-p-acl-mpls-rsvp
  match access-group name copp-system-p-acl-mac-l3-isis
  match access-group name copp-system-p-acl-mac-otv-isis
  match access-group name copp-system-p-acl-mac-fabricpath-isis
  match protocol mpls router-alert
  match protocol mpls exp 6

```



Note The LISP, LISP6, and MAC Layer 3 IS-IS ACLs were added in Cisco NX-OS Release 6.1.

The copp-system-class-important class has the following configuration:

```
ip access-list copp-system-p-acl-hsrp
  permit udp any 224.0.0.2/32 eq 1985
  permit udp any 224.0.0.102/32 eq 1985
```



Note Beginning with Cisco NX-OS Release 6.2(2), the HSRP control packets use predefined destination addresses, as shown above. In Cisco NX-OS releases prior to 6.2(2), the Hot Standby Router Protocol (HSRP) ACL has a lenient entry, with the last octet ignored, as shown in the following configuration:

```
ip access-list copp-system-p-acl-hsrp
  permit udp any 224.0.0.0/24 eq 1985

ipv6 access-list copp-system-p-acl-hsrp6
  permit udp any ff02::66/128 eq 2029

ip access-list copp-system-p-acl-vrrp
  permit ip any 224.0.0.18/32

ip access-list copp-system-p-acl-glbp
  permit udp any eq 3222 224.0.0.0/24 eq 3222

ip access-list copp-system-p-acl-pim-reg
  permit pim any any

ipv6 access-list copp-system-p-acl-icmp6-msgs
  permit icmp any any router-advertisement
  permit icmp any any router-solicitation
  permit icmp any any nd-na
  permit icmp any any nd-ns
  permit icmp any any mld-query
  permit icmp any any mld-report
  permit icmp any any mld-reduction
  permit icmp any any 143

ip access-list copp-system-p-acl-cts
  permit tcp any any eq 64999
  permit tcp any eq 64999 any

ip access-list copp-system-p-acl-pim-mdt-join
  permit udp any 224.0.0.13/32

ipv6 access-list copp-system-p-acl-vrrp6
  permit ipv6 any ff02::12/128

ip access-list copp-system-p-acl-wccp
  permit udp any eq 2048 any eq 2048

mac access-list copp-system-p-acl-mac-lldp
  permit any 0180.c200.000c 0000.0000.0000 0x88cc

mac access-list copp-system-p-acl-mac-flow-control
  permit any 0180.c200.0001 0000.0000.0000 0x8808
```

```

class-map type control-plane match-any copp-system-p-class-important
  match access-group name copp-system-p-acl-cts
  match access-group name copp-system-p-acl-glbp
  match access-group name copp-system-p-acl-hsrp
  match access-group name copp-system-p-acl-vrrp
  match access-group name copp-system-p-acl-wccp
  match access-group name copp-system-p-acl-hsrp6
  match access-group name copp-system-p-acl-vrrp6
  match access-group name copp-system-p-acl-mac-lldp
  match access-group name copp-system-p-acl-mac-flow-control

```



Note The "permit icmp any any 143" rule was added to the acl-icmp6-msgs ACL to support the MLDv2 report in Cisco NX-OS Release 6.1.



Note The VRRP6 ACL was added in Cisco NX-OS Release 6.2(2).



Note Beginning with Cisco NX-OS Release 6.2(2), the behavior of multicast traffic has changed from being policed at different rates in different classes to being grouped into three classes (multicast-host, multicast-router, and normal) and policed at consistent rates, depending on the type of multicast traffic, as follows:

```

ip access-list copp-system-p-acl-igmp
  permit igmp any 224.0.0.0/3
ipv6 access-list copp-system-p-acl-mld
  permit icmp any any mld-query
  permit icmp any any mld-report
  permit icmp any any mld-reduction
  permit icmp any any 143
ip access-list copp-system-p-acl-msdp
  permit tcp any gt 1024 any eq 639
  permit tcp any eq 639 any gt 1024
ipv6 access-list copp-system-p-acl-ndp
  permit icmp any any router-solicitation
  permit icmp any any router-advertisement
  permit icmp any any 137
  permit icmp any any nd-ns
  permit icmp any any nd-na
ip access-list copp-system-p-acl-pim
  permit pim any 224.0.0.0/24
  permit udp any any eq 496
  permit ip any 224.0.0.13/32
ip access-list copp-system-p-acl-pim-mdt-join
  permit udp any 224.0.0.13/32
ip access-list copp-system-p-acl-pim-reg
  permit pim any any
ipv6 access-list copp-system-p-acl-pim6
  permit pim any ff02::d/128
  permit udp any any eq 496
ipv6 access-list copp-system-p-acl-pim6-reg
  permit pim any any
mac access-list copp-system-p-acl-mac-dot1x
  permit any 0180.c200.0003 0000.0000.0000 0x888e
class-map type control-plane match-any copp-system-p-class-multicast-host
  match access-group name copp-system-p-acl-mld

```

```
match access-group name copp-system-p-acl-igmp
class-map type control-plane match-any copp-system-p-class-multicast-router
match access-group name copp-system-p-acl-pim
match access-group name copp-system-p-acl-msdp
match access-group name copp-system-p-acl-pim6
match access-group name copp-system-p-acl-pim-reg
match access-group name copp-system-p-acl-pim6-reg
match access-group name copp-system-p-acl-pim-mdt-join
class-map type control-plane match-any copp-system-p-class-ndp
match access-group name copp-system-p-acl-ndp
```

The `copp-system-class-management` class has the following configuration:

```
ip access-list copp-system-p-acl-tacacs
  permit tcp any any eq tacacs
  permit tcp any eq tacacs any

ip access-list copp-system-p-acl-radius
  permit udp any any eq 1812
  permit udp any any eq 1813
  permit udp any any eq 1645
  permit udp any any eq 1646
  permit udp any eq 1812 any
  permit udp any eq 1813 any
  permit udp any eq 1645 any
  permit udp any eq 1646 any

ip access-list copp-system-p-acl-ntp
  permit udp any any eq ntp

ip access-list copp-system-p-acl-ftp
  permit tcp any any eq ftp-data
  permit tcp any any eq ftp
  permit tcp any eq ftp-data any
  permit tcp any eq ftp any

ip access-list copp-system-p-acl-tftp
  permit udp any any eq tftp
  permit udp any any eq 1758
  permit udp any eq tftp any
  permit udp any eq 1758 any

ip access-list copp-system-p-acl-sftp
  permit tcp any any eq 115
  permit tcp any eq 115 any

ip access-list copp-system-p-acl-ssh
  permit tcp any any eq 22
  permit tcp any eq 22 any

ip access-list copp-system-p-acl-snmp
  permit udp any any eq snmp
  permit udp any any eq snmptrap

ip access-list copp-system-p-acl-telnet
  permit tcp any any eq telnet
  permit tcp any any eq 107
  permit tcp any eq telnet any
  permit tcp any eq 107 any

ipv6 access-list copp-system-p-acl-tacacs6
  permit tcp any any eq tacacs
  permit tcp any eq tacacs any
```

```

ipv6 access-list copp-system-p-acl-radius6
  permit udp any any eq 1812
  permit udp any any eq 1813
  permit udp any any eq 1645
  permit udp any any eq 1646
  permit udp any eq 1812 any
  permit udp any eq 1813 any
  permit udp any eq 1645 any
  permit udp any eq 1646 any

ipv6 access-list copp-system-p-acl-ntp6
  permit udp any any eq ntp
  permit udp any eq ntp any

ipv6 access-list copp-system-p-acl-tftp6
  permit udp any any eq tftp
  permit udp any any eq 1758
  permit udp any eq tftp any
  permit udp any eq 1758 any

ipv6 access-list copp-system-p-acl-ssh6
  permit tcp any any eq 22
  permit tcp any eq 22 any

ipv6 access-list copp-system-p-acl-telnet6
  permit tcp any any eq telnet
  permit tcp any any eq 107
  permit tcp any eq telnet any
  permit tcp any eq 107 any

class-map type control-plane match-any copp-system-p-class-management
  match access-group name copp-system-p-acl-tacacs
  match access-group name copp-system-p-acl-radius
  match access-group name copp-system-p-acl-ntp
  match access-group name copp-system-p-acl-ftp
  match access-group name copp-system-p-acl-tftp
  match access-group name copp-system-p-acl-sftp
  match access-group name copp-system-p-acl-ssh
  match access-group name copp-system-p-acl-snmp
  match access-group name copp-system-p-acl-telnet
  match access-group name copp-system-p-acl-tacacs6
  match access-group name copp-system-p-acl-radius6
  match access-group name copp-system-p-acl-ntp6
  match access-group name copp-system-p-acl-tftp6
  match access-group name copp-system-p-acl-ssh6
  match access-group name copp-system-p-acl-telnet6

```

The `copp-system-class-normal` class has the following configuration:

```

ip access-list copp-system-p-acl-dhcp
  permit udp any neq bootps any eq bootps
  permit udp any eq bootpc any

ip access-list copp-system-p-acl-dhcp-relay-response
  permit udp any eq bootps any
  permit udp any any eq bootpc

mac access-list copp-system-p-acl-mac-dot1x
  permit any 0180.c200.0003 0000.0000.0000 0x888e

class-map type control-plane match-any copp-system-p-class-normal
  match access-group name copp-system-p-acl-mac-dot1x
  match exception multicast directly-connected-sources

```

```

match protocol arp

class-map type control-plane match-any copp-system-p-class-normal-dhcp
match redirect dhcp-snoop
match access-group name copp-system-p-acl-dhcp

class-map type control-plane match-any copp-system-p-class-normal-dhcp-relay-response
match access-group name copp-system-p-acl-dhcp-relay-response

```

The `copp-system-class-redirect` class has the following configuration:

```

class-map type control-plane match-any copp-system-p-class-redirect
match redirect arp-inspect

```

The `copp-system-class-monitoring` class has the following configuration:

```

ip access-list copp-system-p-acl-icmp
permit icmp any any echo
permit icmp any any echo-reply

ip access-list copp-system-p-acl-traceroute
permit icmp any any ttl-exceeded
permit icmp any any port-unreachable
permit udp any any range 33434 33534

ipv6 access-list copp-system-p-acl-icmp6
permit icmp any any echo-request
permit icmp any any echo-reply

class-map type control-plane match-any copp-system-p-class-monitoring
match access-group name copp-system-p-acl-icmp
match access-group name copp-system-p-acl-traceroute
match access-group name copp-system-p-acl-icmp6

```

The `copp-system-class-l2-unpoliced` class has the following configuration:

```

mac access-list copp-system-p-acl-mac-cdp-udld-vtp
permit any 0100.0ccc.cccc 0000.0000.0000

mac access-list copp-system-p-acl-mac-stp
permit any 0100.0ccc.cccd 0000.0000.0000
permit any 0180.c200.0000 0000.0000.0000

mac access-list copp-system-p-acl-mac-lacp
permit any 0180.c200.0002 0000.0000.0000 0x8809

mac access-list copp-system-p-acl-mac-cfsoe
permit any 0180.C200.000E 0000.0000.0000 0x8843

mac access-list copp-system-p-acl-mac-l2-tunnel
permit any any 0x8840

class-map type control-plane copp-system-p-class-l2-unpoliced
match access-group name copp-system-p-acl-mac-stp
match access-group name copp-system-p-acl-mac-lacp
match access-group name copp-system-p-acl-mac-cfsoe
match access-group name copp-system-p-acl-mac-sdp-srp
match access-group name copp-system-p-acl-mac-l2-tunnel

```



Note The MAC Layer 2 tunnel ACL was added in Cisco NX-OS Release 6.1.

The `copp-system-class-l2-default` class has the following configuration:

```
mac access-list copp-system-p-acl-mac-undesirable
  permit any any

class-map type control-plane copp-system-p-class-l2-default
  match access-group name copp-system-p-acl-mac-undesirable
  match protocol mpls
```

The `copp-system-class-fcoe` class has the following configuration:

```
mac access-list copp-system-p-acl-mac-fcoe
  permit any any 0x8906
  permit any any 0x8914

class-map type control-plane match-any copp-system-p-class-fcoe
  match access-group name copp-system-p-acl-mac-fcoe
```



Note The `copp-system-class-fcoe` class was added in Cisco NX-OS Release 6.1.

The `copp-system-class-undesirable` class has the following configuration:

```
ip access-list copp-system-p-acl-undesirable
  permit udp any any eq 1434

class-map type control-plane match-any copp-system-p-class-undesirable
  match access-group name copp-system-p-acl-undesirable
  match exception fcoe-fib-miss
```



Note The `fcoe-fib-miss` match exception was added in Cisco NX-OS Release 6.1.

```
mac access-list copp-system-acl-mac-cdp-udld-vtp
  permit any 0100.0ccc.cccc 0000.0000.0000
mac access-list copp-system-acl-mac-cfsoe
  permit any 0180.c200.000e 0000.0000.0000 0x8843
mac access-list copp-system-acl-mac-dot1x
  permit any 0180.c200.0003 0000.0000.0000 0x888e
mac access-list copp-system-acl-mac-flow-control
  permit any 0180.c200.0001 0000.0000.0000 0x8808
mac access-list copp-system-acl-mac-l2mp-isis
  permit any 0180.c200.0015 0000.0000.0000
  permit any 0180.c200.0014 0000.0000.0000
mac access-list copp-system-acl-mac-l2pt
  permit any 0100.0ccd.cdd0 0000.0000.0000
mac access-list copp-system-acl-mac-lacp
  permit any 0180.c200.0002 0000.0000.0000 0x8809
```

```
mac access-list copp-system-acl-mac-lldp
  permit any 0180.c200.000e 0000.0000.0000 0x88c
mac access-list copp-system-acl-mac-stp
  permit any 0100.0ccc.cccd 0000.0000.0000
  permit any 0180.c200.0000 0000.0000.0000
mac access-list copp-system-acl-mac-undesirable
  permit any any
```

Strict Default CoPP Policy

The strict CoPP policy has the following configuration:

```
policy-map type control-plane copp-system-p-policy-strict

  class copp-system-p-class-critical
    set cos 7
    police cir 36000 kbps bc 250 ms conform transmit violate drop

  class copp-system-p-class-important
    set cos 6
    police cir 1400 kbps bc 1500 ms conform transmit violate drop

  class copp-system-p-class-multicast-router
    set cos 6
    police cir 2600 kbps bc 1000 ms conform transmit violate drop

  class copp-system-p-class-management
    set cos 2
    police cir 10000 kbps bc 250 ms conform transmit violate drop

  class copp-system-p-class-multicast-host
    set cos 1
    police cir 1000 kbps bc 1000 ms conform transmit violate drop

  class copp-system-p-class-normal
    set cos 1
    police cir 680 kbps bc 250 ms conform transmit violate drop

  class copp-system-p-class-ndp
    set cos 6
    police cir 680 kbps bc 250 ms conform transmit violate drop

  class copp-system-p-class-normal-dhcp
    set cos 1
    police cir 1500 kbps bc 250 ms conform transmit violate drop

  class copp-system-p-class-normal-dhcp-relay-response
    set cos 1
    police cir 1800 kbps bc 500 ms conform transmit violate drop

  class copp-system-p-class-redirect
    set cos 1
    police cir 280 kbps bc 250 ms conform transmit violate drop

  class copp-system-p-class-exception
    set cos 1
    police cir 360 kbps bc 250 ms conform transmit violate drop

  class copp-system-p-class-monitoring
    set cos 1
    police cir 130 kbps bc 1000 ms conform transmit violate drop
```

```

class copp-system-p-class-l2-unpoliced
  police cir 8 gbps bc 5 mbytes conform transmit violate transmit

class copp-system-p-class-undesirable
  set cos 0
  police cir 32 kbps bc 250 ms conform drop violate drop

class copp-system-p-class-fcoe
  set cos 6
  police cir 1060 kbps bc 1000 ms conform transmit violate drop

class copp-system-p-class-l2-default
  police cir 10 kbps bc 250 ms conform transmit violate drop

class class-default
  set cos 0
  police cir 10 kbps bc 250 ms conform transmit violate drop

```



Note The `copp-system-p-class-fcoe` class was added in Cisco NX-OS Release 6.1. The `copp-system-p-class-multicast-router` and `copp-system-p-class-multicast-host` classes were added in Cisco NX-OS Release 6.2(2).

Moderate Default CoPP Policy

The moderate CoPP policy has the following configuration:

```

policy-map type control-plane copp-system-p-policy-moderate

  class copp-system-p-class-critical
    set cos 7
    police cir 36000 kbps bc 310 ms conform transmit violate drop

  class copp-system-p-class-important
    set cos 6
    police cir 1400 kbps bc 1250 ms conform transmit violate drop

  class copp-system-p-class-multicast-router
    set cos 6
    police cir 2600 kbps bc 1000 ms conform transmit violate drop

  class copp-system-p-class-management
    set cos 2
    police cir 10000 kbps bc 310 ms conform transmit violate drop

  class copp-system-p-class-multicast-host
    set cos 1
    police cir 1000 kbps bc 1000 ms conform transmit violate drop

  class copp-system-p-class-normal
    set cos 1
    police cir 680 kbps bc 310 ms conform transmit violate drop

  class copp-system-p-class-ndp
    set cos 6
    police cir 680 kbps bc 310 ms conform transmit violate drop

  class copp-system-p-class-normal-dhcp
    set cos 1

```

```

    police cir 1500 kbps bc 310 ms conform transmit violate drop

class copp-system-p-class-normal-dhcp-relay-response
    set cos 1
    police cir 1800 kbps bc 620 ms conform transmit violate drop

class copp-system-p-class-redirect
    set cos 1
    police cir 280 kbps bc 310 ms conform transmit violate drop

class copp-system-p-class-exception
    set cos 1
    police cir 360 kbps bc 310 ms conform transmit violate drop

class copp-system-p-class-monitoring
    set cos 1
    police cir 130 kbps bc 1250 ms conform transmit violate drop

class copp-system-p-class-l2-unpoliced
    police cir 8 gbps bc 5 mbytes conform transmit violate transmit

class copp-system-p-class-undesirable
    set cos 0
    police cir 32 kbps bc 310 ms conform drop violate drop

class copp-system-p-class-fcoe
    set cos 6
    police cir 1060 kbps bc 1250 ms conform transmit violate drop

class copp-system-p-class-l2-default
    police cir 10 kbps bc 310 ms conform transmit violate drop

class class-default
    set cos 0
    police cir 10 kbps bc 250 ms conform transmit violate drop

```



Note The `copp-system-p-class-fcoe` class was added in Cisco NX-OS Release 6.1. The `copp-system-p-class-multicast-router` and `copp-system-p-class-multicast-host` classes were added in Cisco NX-OS Release 6.2(2).

Lenient Default CoPP Policy

The lenient CoPP policy has the following configuration:

```

policy-map type control-plane copp-system-p-policy-lenient

class copp-system-p-class-critical
    set cos 7
    police cir 36000 kbps bc 375 ms conform transmit violate drop

class copp-system-p-class-important
    set cos 6
    police cir 1400 kbps bc 1500 ms conform transmit violate drop

class copp-system-p-class-multicast-router
    set cos 6
    police cir 2600 kbps bc 1000 ms conform transmit violate drop

```

```

class copp-system-p-class-management
  set cos 2
  police cir 10000 kbps bc 375 ms conform transmit violate drop

class copp-system-p-class-multicast-host
  set cos 1
  police cir 1000 kbps bc 1000 ms conform transmit violate drop

class copp-system-p-class-normal
  set cos 1
  police cir 680 kbps bc 375 ms conform transmit violate drop

class copp-system-p-class-ndp
  set cos 6
  police cir 680 kbps bc 375 ms conform transmit violate drop

class copp-system-p-class-normal-dhcp
  set cos 1
  police cir 1500 kbps bc 375 ms conform transmit violate drop

class copp-system-p-class-normal-dhcp-relay-response
  set cos 1
  police cir 1800 kbps bc 750 ms conform transmit violate drop

class copp-system-p-class-redirect
  set cos 1
  police cir 280 kbps bc 375 ms conform transmit violate drop

class copp-system-p-class-exception
  set cos 1
  police cir 360 kbps bc 375 ms conform transmit violate drop

class copp-system-p-class-monitoring
  set cos 1
  police cir 130 kbps bc 1500 ms conform transmit violate drop

class copp-system-p-class-l2-unpoliced
  police cir 8 gbps bc 5 mbytes conform transmit violate transmit

class copp-system-p-class-undesirable
  set cos 0
  police cir 32 kbps bc 375 ms conform drop violate drop

class copp-system-p-class-fcoe
  set cos 6
  police cir 1060 kbps bc 1500 ms conform transmit violate drop

class copp-system-p-class-l2-default
  police cir 10 kbps bc 375 ms conform transmit violate drop

class class-default
  set cos 0
  police cir 10 kbps bc 250 ms conform transmit violate drop

```



Note The `copp-system-p-class-fcoe` class was added in Cisco NX-OS Release 6.1. The `copp-system-p-class-multicast-router` and `copp-system-p-class-multicast-host` classes were added in Cisco NX-OS Release 6.2(2).

Dense Default CoPP Policy

The dense CoPP policy has the following configuration in Cisco NX-OS Release 6.2(2):

```

policy-map type control-plane copp-system-p-policy-dense
  class copp-system-p-class-critical
    set cos 7
    police cir 4500 kbps bc 250 ms conform transmit violate drop
  class copp-system-p-class-important
    set cos 6
    police cir 1400 kbps bc 1500 ms conform transmit violate drop
  class copp-system-p-class-multicast-router
    set cos 6
    police cir 370 kbps bc 1000 ms conform transmit violate drop
  class copp-system-p-class-management
    set cos 2
    police cir 2500 kbps bc 1000 ms conform transmit violate drop
  class copp-system-p-class-multicast-host
    set cos 1
    police cir 190 kbps bc 1000 ms conform transmit violate drop
  class copp-system-p-class-normal
    set cos 1
    police cir 300 kbps bc 250 ms conform transmit violate drop
  class copp-system-p-class-ndp
    set cos 6
    police cir 300 kbps bc 250 ms conform transmit violate drop
  class copp-system-p-class-normal-dhcp
    set cos 1
    police cir 660 kbps bc 1000 ms conform transmit violate drop
  class copp-system-p-class-normal-dhcp-relay-response
    set cos 1
    police cir 800 kbps bc 1000 ms conform transmit violate drop
  class copp-system-p-class-redirect
    set cos 1
    police cir 200 kbps bc 250 ms conform transmit violate drop
  class copp-system-p-class-exception
    set cos 1
    police cir 200 kbps bc 250 ms conform transmit violate drop
  class copp-system-p-class-monitoring
    set cos 1
    police cir 130 kbps bc 1000 ms conform transmit violate drop
  class copp-system-p-class-l2-unpoliced
    police cir 8 gbps bc 5 mbytes conform transmit violate transmit
  class copp-system-p-class-undesirable
    set cos 0
    police cir 32 kbps bc 250 ms conform drop violate drop
  class copp-system-p-class-fcoe
    set cos 6
    police cir 600 kbps bc 1000 ms conform transmit violate drop
  class copp-system-p-class-l2-default
    police cir 10 kbps bc 250 ms conform transmit violate drop
  class class-default
    set cos 0
    police cir 10 kbps bc 250 ms conform transmit violate drop

```



Note The `copp-system-p-class-fcoe` class was added in Cisco NX-OS Release 6.1. The `copp-system-p-class-multicast-router` and `copp-system-p-class-multicast-host` classes were added in Cisco NX-OS Release 6.2(2).

Packets Per Second Credit Limit

The aggregate packets per second (PPS) for a given policy (sum of PPS of each class part of the policy) is capped by an upper PPS Credit Limit (PCL). If an increase in PPS of a given class causes a PCL exceed, the configuration is rejected. To increase the desired PPS, the additional PPS beyond PCL should be decreased from other class(es).

Modular QoS Command-Line Interface

CoPP uses the Modular Quality of Service Command-Line Interface (MQC). MQC is a CLI structure that allows you to define a traffic class, create a traffic policy (policy map), and attach the traffic policy to an interface. The traffic policy contains the CoPP feature that will be applied to the traffic class.

SUMMARY STEPS

1. Define a traffic class using the **class-map** command. A traffic class is used to classify traffic.
2. Create a traffic policy using the **policy-map** command. A traffic policy (policy map) contains a traffic class and one or more CoPP features that will be applied to the traffic class. The CoPP features in the traffic policy determine how to treat the classified traffic.
3. Attach the traffic policy (policy map) to the control plane using the **control-plane** and **service-policy** commands.

DETAILED STEPS

Step 1 Define a traffic class using the **class-map** command. A traffic class is used to classify traffic.

This example shows how to create a new class-map called copp-sample-class:

```
class-map type control-plane copp-sample-class
```

Step 2 Create a traffic policy using the **policy-map** command. A traffic policy (policy map) contains a traffic class and one or more CoPP features that will be applied to the traffic class. The CoPP features in the traffic policy determine how to treat the classified traffic.

Step 3 Attach the traffic policy (policy map) to the control plane using the **control-plane** and **service-policy** commands.

This example shows how to attach the policy map to the control plane:

```
control-plane
service-policy input copp-system-policy
```

Note The copp-system-policy is always configured and applied. There is no need to use this command explicitly.

CoPP and the Management Interface

The Cisco NX-OS device supports only hardware-based CoPP which does not support the management interface (mgmt0). The out-of-band mgmt0 interface connects directly to the CPU and does not pass through the in-band traffic hardware where CoPP is implemented.

On the mgmt0 interface, ACLs can be configured to give or deny access to a particular type of traffic.

Related Topics

[Configuring IP ACLs](#)

[Configuring MAC ACLs](#)

Virtualization Support for CoPP

You can configure CoPP in the default virtual device context (VDC) or the admin VDC, but the CoPP configuration applies to all VDCs on the Cisco NX-OS device. For more information on VDCs, see the *Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*.

Guidelines and Limitations for CoPP

CoPP has the following configuration guidelines and limitations:

- Support for uRPF exception CoPP class is introduced in Cisco NX-OS Release 8.2(6). By default all uRPF exception packets are punted to the supervisor module. A new CoPP class, **copp-system-p-classurpf-exception** is introduced to match uRPF exception packets and police them at 100 kbps. You can customize the default CoPP profiles and you can choose to drop uRPF exceptions or police at a lower rate.
- CoPP classification does not work for the Layer 2 control traffic in native VLAN in the following scenarios:
 - When the **native vlan** (ID other than 1) command is configured on the interface and the native VLAN ID is missing in the configuration.
 - If the **vlan dot1q tag native exclude control command** is configured.
- We recommend that you use the strict default CoPP policy initially and then later modify the CoPP policies based on the data center and application requirements.
- We recommend applying the default dense policy when the chassis is fully loaded with F2 or F2e Series modules or loaded with more F2 or F2e Series modules than any other type of I/O module.
- We recommend configuring the scale factor and applying the default dense policy when the chassis is loaded with both F2 or F2e and M Series modules.
- Customizing CoPP is an ongoing process. CoPP must be configured according to the protocols and features used in your specific environment as well as the supervisor features that are required by the server environment. As these protocols and features change, CoPP must be modified.
- We recommend that you continuously monitor CoPP. If drops occur, determine if CoPP dropped traffic unintentionally or in response to a malfunction or attack. In either event, analyze the situation and evaluate the need to modify the CoPP policies.
- All the traffic that you do not specify in the other class maps is put into the last class, the default class. Monitor the drops in this class and investigate if these drops are based on traffic that you do not want or the result of a feature that was not configured and you need to add.
- All broadcast traffic is sent through CoPP logic in order to determine which packets (for example, ARP and DHCP) need to be redirected through an access control list (ACL) to the router processor. Broadcast traffic that does not need to be redirected is matched against the CoPP logic, and both conforming and

violated packets are counted in the hardware but not sent to the CPU. Broadcast traffic that needs to be sent to the CPU and broadcast traffic that does not need to be sent to the CPU must be separated into different classes.

- When you configure a policer in a CoPP class map active policy with a valid CIR value, but both conform and violate action is set to drop the packets, the CIR value will be taken as 0. The configuration of **conform drop violate drop** action drops all the classified packets irrespective of the incoming rate.

Thus, as expected all packets will be dropped and the CoPP statistics will display the conformed counter as "0 bytes" and will not be incremented. This is an expected behaviour.

- In a CoPP policy-map, make sure you set the class with police rate as bps (bytes per second) and not as pps (packets per second). The Control plane policy segregates different packets destined for the control plane into different classes. Using hardware policers, you can define separate actions for traffic that conforms to, exceeds, or violates certain conditions. The actions can transmit the packet, mark down the packet, or drop the packet.

The **police [cir] {cir-rate [bps | gbps | kbps | mbps | pps]}** command allows you to configure the policer CIR unit in bps. But the Cisco Nexus 7000 hardware considers the byte-policing rather than the packet-policing. Therefore, you are suggested to use bps and not pps when you set the class with the police rate.

- If you remove the **set cos** configuration, there is a difference in behavior between M1 Series modules and F2/F2e Series modules with SVI and trunk ports. With an M1 Series module, when Layer 3 control packets with both DSCP and UserPriority (UP) (in the VLAN header) are received, queuing is performed using DSCP. With a F2/F2e Series module, queuing is performed using UP.
- In Cisco NX-OS releases prior to 5.2, you must use the setup utility to change or reapply the default copp-system-policy policy. You can access the setup utility using the **setup** command in the CLI.
- After you have configured CoPP, delete anything that is not being used, such as old class maps and unused routing protocols.
- You must ensure that the CoPP policy does not filter critical traffic such as routing protocols or interactive access to the device. Filtering this traffic could prevent remote access to the Cisco NX-OS device and require a console connection.
- The Cisco NX-OS software does not support egress CoPP or silent mode. CoPP is supported only on ingress (you cannot use the **service-policy output copp** command to the control plane interface).
- You can use the access control entry (ACE) hit counters in the hardware only for ACL logic. Use the software ACE hit counters and the **show access-lists** and **show policy-map type control-plane** commands to evaluate CPU traffic.
- The Cisco NX-OS device hardware performs CoPP on a per-forwarding-engine basis. CoPP does not support distributed policing. Therefore, you should choose rates so that the aggregate traffic does not overwhelm the supervisor module.
- To get a more granular view of traffic that reaches the supervisor and might be dropped by CoPP, you can use the NetFlow feature on SVIs. To do so, compare the ACL hit counts by the values listed in the NetFlow table.
- F1 Series modules do not support CoPP.
- In Cisco NX-OS Release 5.0, CoPP does not support non-IP traffic classification. Instead, you can use ACLs to drop or limit the non-IP traffic that reaches the supervisor module.

- The following rules apply beginning with Cisco NX-OS Release 5.1: The following rules apply for Cisco NX-OS Release 4.2(6):
 - CoPP supports non-IP and IP traffic classes.
 - L2PT, OTV-ISIS, and FabricPath-ISIS packets are classified under the `copp-system-class-critical` policy.
 - LLDP and flow-control packets are classified under the `copp-system-class-important` policy.
 - Dot1x packets are classified under the `copp-system-class-normal` policy.
 - STP, CDP, UDLD, VTP, LACP, and CFSOE packets are classified under the `copp-system-class-l2-unpoliced` policy. These packets are only classified; they are not policed. The corresponding policer simply displays the statistics. These packets are always forwarded to the supervisor.
 - The rest of the non-IP traffic is classified under the `copp-system-class-l2-default` policy.
 - IP traffic not matching any of the copp classes is classified under the `class-default` policy.
- CoPP MAC policies are supported beginning with Cisco NX-OS Release 5.1.
- If you use the in-service software grade (ISSU) to upgrade to Cisco NX-OS Release 5.1, the default CoPP policies for the following features must be manually configured: FabricPath, OTV, L2PT, LLDP, DHCP, and DOT1X.
- Beginning with Cisco NX-OS Release 5.2, the CoPP best practice policy is read-only. If you want to modify its configuration, you must copy it. Copied policies are treated as user configurations.
- When you use ISSU to upgrade to Cisco NX-OS Release 5.2, the policy attached to the control plane is treated as a user-configured policy. Check the CoPP profile using the `show copp profile` command and make any required changes.
- If you use the in-service software downgrade (ISSD) to downgrade from Cisco NX-OS Release 5.2, CoPP reports the incompatible configuration and instructs you to copy the CoPP profile. In the lower version, all configurations are restored in user-configuration mode.
- If you downgrade from Cisco NX-OS Release 5.2 without using ISSD, the CoPP configuration is lost, and a CoPP policy is no longer attached to the control plane.
- When you use ISSU to upgrade to a new Cisco NX-OS release, the default CoPP policy for the new release is not applied. Because you might have your own configured CoPP policy and want to continue using it, the policy for the prior release continues to be applied. However, if you have not modified the default CoPP policy in prior versions, we recommend that when you install Cisco NX-OS Release 5.2 or later releases, you apply the latest default CoPP policy for that version by using the `copp profile [strict | moderate | lenient]` command. This action removes the previous policy and applies the new one.
- Beginning with Cisco NX-OS Release 5.2, the default CoPP policies are read only. To make modifications, copy the default profile by using the `copp copy profile {strict | moderate | lenient} {prefix | suffix} string`, make modifications, and then apply that policy to the control plane using the `service-policy input policy-map-name` command.
- If multiple flows map to the same class, individual flow statistics will not be available.
- Support for monitoring CoPP with SNMP is limited to the listed cbQoS MIB tables and the elements attached to the control plane.



Note If you are familiar with the Cisco IOS CLI, be aware that the Cisco NX-OS commands for this feature might differ from the Cisco IOS commands that you would use.

Default Settings for CoPP

This table lists the default settings for CoPP parameters.

Table 1: Default CoPP Parameters Settings

Parameters	Default
Default policy	Strict
Default policy	9 policy entries Note The maximum number of supported policies with associated class maps is 128.
Scale factor value	1.00

Configuring CoPP

This section describes how to configure CoPP.

Configuring a Control Plane Class Map

You must configure control plane class maps for control plane policies.

You can classify traffic by matching packets based on existing ACLs. The permit and deny ACL keywords are ignored in the matching.

You can configure policies for IP version 4 (IPv4) and IP version 6 (IPv6) packets.

Before you begin

Ensure that you are in the default VDC.

Ensure that you have configured the IP ACLs if you want to use ACE hit counters in the class maps.

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **class-map type control-plane [match-all | match-any] class-map-name**
3. (Optional) switch(config-cmap)# **match access-group name access-list-name**
4. (Optional) switch(config-cmap)# **match exception {ip | ipv6} icmp redirect**
5. (Optional) switch(config-cmap)# **match exception {ip | ipv6} icmp unreachable**

6. (Optional) switch(config-cmap)# **match exception {ip | ipv6} option**
7. (Optional) switch(config-cmap)# **match exception {ip | ipv6} unicast rpf-failure**
8. switch(config-cmap)# **match protocol arp**
9. (Optional) switch(config-cmap)# **match redirect arp-inspect**
10. (Optional) switch(config-cmap)# **match redirect dhcp-snoop**
11. switch(config-cmap)# **exit**
12. (Optional) switch(config)# **show class-map type control-plane [class-map-name]**
13. (Optional) switch(config)# **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	switch# configure terminal	Enters global configuration mode.
Step 2	switch(config)# class-map type control-plane [match-all match-any] class-map-name	Specifies a control plane class map and enters class map configuration mode. The default class matching is match-any. The name can be a maximum of 64 characters long and is case sensitive. Note You cannot use class-default, match-all, or match-any as class map names.
Step 3	(Optional) switch(config-cmap)# match access-group name access-list-name	Specifies matching for an IP ACL. Note The permit and deny ACL keywords are ignored in the CoPP matching.
Step 4	(Optional) switch(config-cmap)# match exception {ip ipv6} icmp redirect	Specifies matching for IPv4 or IPv6 ICMP redirect exception packets.
Step 5	(Optional) switch(config-cmap)# match exception {ip ipv6} icmp unreachable	Specifies matching for IPv4 or IPv6 ICMP unreachable exception packets.
Step 6	(Optional) switch(config-cmap)# match exception {ip ipv6} option	Specifies matching for IPv4 or IPv6 option exception packets.
Step 7	(Optional) switch(config-cmap)# match exception {ip ipv6} unicast rpf-failure	Specifies matching for IPv4 or IPv6 Unicast Reverse Path Forwarding (Unicast RPF) exception packets. For any CoPP class map, you can rate limit the IPv4 or IPv6 URPF exception packets as per the class map's rate limit configuration.
Step 8	switch(config-cmap)# match protocol arp	Specifies matching for IP Address Resolution Protocol (ARP) and Reverse Address Resolution Protocol (RARP) packets.
Step 9	(Optional) switch(config-cmap)# match redirect arp-inspect	Specifies matching for ARP inspection redirected packets.
Step 10	(Optional) switch(config-cmap)# match redirect dhcp-snoop	Specifies matching for Dynamic Host Configuration Protocol (DHCP) snooping redirected packets.

	Command or Action	Purpose
Step 11	switch(config-cmap)# exit	Exits class map configuration mode.
Step 12	(Optional) switch(config)# show class-map type control-plane [<i>class-map-name</i>]	Displays the control plane class map configuration.
Step 13	(Optional) switch(config)# copy running-config startup-config	Copies the running configuration to the startup configuration.

Configuring a Control Plane Policy Map

You must configure a policy map for CoPP, which includes policing parameters. If you do not configure a policer for a class, the default policer conform action is drop. The Cisco NX-OS software supports 1-rate 2-color and 2-rate 3-color policing.

The **policy-map** command is used to associate a traffic class, defined by the **class-map** command, with one or more QoS policies. The result of this association is called a service policy. A service policy contains three elements: a name, a traffic class (specified with the **class** command), and the QoS policies. The purpose of the service policy is to associate a traffic class with one or more QoS policies. Classes included within policy maps are processed top-down. When a packet is found to match a class, no further processing is performed. That is, a packet can only belong to a single class, and it is the first one to which a match occurs. When a packet does not match any of the defined classes, it is automatically placed in the class **class-default**. The default class is always applied, whether it is explicitly configured or not.

Before you begin

Ensure that you are in the default VDC.

Ensure that you have configured a control plane class map.

SUMMARY STEPS

- 1. configure terminal**
- 2. policy-map type control-plane** *policy-map-name*
- 3. class** {*class-map-name* [**insert-before** *class-map-name2*] | **class-default**}
- 4. police** [**cir**] {*cir-rate* [**bps** | **gbps** | **kbps** | **mbps** | **pps**]}
- 5. police** [**cir**] {*cir-rate* [**bps** | **gbps** | **kbps** | **mbps** | **pps**] [**bc**] *burst-size* [**bytes** | **kbytes** | **mbytes** | **ms** | **packets** | **us**]}
- 6. police** [**cir**] {*cir-rate* [**bps** | **gbps** | **kbps** | **mbps** | **pps**] **conform** {**drop** | **set-cos-transmit** *cos-value* | **set-dscp-transmit** *dscp-value* | **set-prec-transmit** *prec-value* | **transmit**} [**exceed** {**drop** | **set dscp dscp table cir-markdown-map** | **transmit**}] [**violate** {**drop** | **set dscp dscp table pir-markdown-map** | **transmit**}]}
- 7. police** [**cir**] {*cir-rate* [**bps** | **gbps** | **kbps** | **mbps** | **pps**] **pir** *pir-rate* [**bps** | **gbps** | **kbps** | **mbps**] [[**be**] *burst-size* [**bytes** | **kbytes** | **mbytes** | **ms** | **packets** | **us**]}
- (Optional) **logging drop threshold** [*drop-count* [**level** *syslog-level*]]
- (Optional) **set cos** [**inner**] *cos-value*
- (Optional) **set dscp** [**tunnel**] {*dscp-value* | **af11** | **af12** | **af13** | **af21** | **af22** | **af23** | **af31** | **af32** | **af33** | **af41** | **af42** | **af43** | **cs1** | **cs2** | **cs3** | **cs4** | **cs5** | **cs6** | **cs7** | **ef** | **default**}
- (Optional) **set precedence** [**tunnel**] {*prec-value* | **critical** | **flash** | **flash-override** | **immediate** | **internet** | **network** | **priority** | **routine**}

12. **exit**
13. **exit**
14. (Optional) **show policy-map type control-plane [expand] [name class-map-name]**
15. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	<p>configure terminal</p> <p>Example:</p> <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
Step 2	<p>policy-map type control-plane <i>policy-map-name</i></p> <p>Example:</p> <pre>switch(config)# policy-map type control-plane ClassMapA switch(config-pmap)#</pre>	Specifies a control plane policy map and enters policy map configuration mode. The policy map name can have a maximum of 64 characters and is case sensitive.
Step 3	<p>class {<i>class-map-name</i> [insert-before <i>class-map-name2</i>] class-default}</p> <p>Example:</p> <pre>switch(config-pmap)# class ClassMapA switch(config-pmap-c)#</pre>	Specifies a control plane class map name or the class default and enters control plane class configuration mode. The class-default class map is always at the end of the class map list for a policy map.
Step 4	<p>police [cir] {<i>cir-rate</i> [bps gbps kbps mbps pps]}</p> <p>Example:</p> <pre>switch(config-pmap-c)# police cir 52000</pre>	Specifies the committed information rate (CIR). The rate range is from 0 to 80000000000. The default CIR unit is bps.
Step 5	<p>police [cir] {<i>cir-rate</i> [bps gbps kbps mbps pps]} [<i>bc</i>] <i>burst-size</i> [bytes kbytes mbytes ms packets us]</p> <p>Example:</p> <pre>switch(config-pmap-c)# police cir 52000 bc 1000</pre>	Specifies the CIR with the committed burst (BC). The CIR range is from 0 to 80000000000 and the BC range is from 0 to 512000000. The default CIR unit is bps and the default BC size unit is bytes.
Step 6	<p>police [cir] {<i>cir-rate</i> [bps gbps kbps mbps pps]} conform {drop set-cos-transmit <i>cos-value</i> set-dscp-transmit <i>dscp-value</i> set-prec-transmit <i>prec-value</i> transmit} [exceed {drop set dscp dscp table <i>cir-markdown-map</i> transmit}] [violate {drop set dscp dscp table <i>pir-markdown-map</i> transmit}]</p> <p>Example:</p> <pre>switch(config-pmap-c)# police cir 52000 conform transmit exceed drop</pre>	<p>Specifies the CIR with the conform action. The CIR range is from 0 to 80000000000. The default rate unit is bps. The range for the <i>cos-value</i> and <i>prec-value</i> arguments is from 0 to 7. The range for the <i>dscp-value</i> argument is from 0 to 63.</p> <p>The options are as follows:</p> <ul style="list-style-type: none"> • drop—Drops the packet. • set-cos-transmit—Sets the class of service (CoS) value. • set-dscp-transmit—Sets the differentiated services code point value.

	Command or Action	Purpose
		<ul style="list-style-type: none"> • set-prec-transmit—Sets the precedence value. • transmit—Transmits the packet. • set dscp dscp table cir-markdown-map—Sets the exceed action to the CIR markdown map. • set dscp dscp table pir-markdown-map—Sets the violate action to the PIR markdown map. <p>Note You can specify the BC and conform action for the same CIR.</p>
Step 7	<p>police [cir] {cir-rate [bps gbps kbps mbps pps]} pir pir-rate [bps gbps kbps mbps] [[be] burst-size [bytes kbytes mbytes ms packets us]]</p> <p>Example:</p> <pre>switch(config-pmap-c)# police cir 52000 pir 78000 be 2000</pre>	<p>Specifies the CIR with the peak information rate (PIR). The CIR range is from 0 to 8000000000 and the PIR range is from 1 to 8000000000. You can optionally set an extended burst (BE) size. The BE range is from 1 to 512000000. The default CIR unit is bps, the default PIR unit is bps, and the default BE size unit is bytes.</p> <p>Note You can specify the BC, conform action, and PIR for the same CIR.</p>
Step 8	<p>(Optional) logging drop threshold [drop-count [level syslog-level]]</p> <p>Example:</p> <pre>switch(config-pmap-c)# logging drop threshold 100</pre>	<p>Specifies the threshold value for dropped packets and generates a syslog if the drop count exceeds the configured threshold. The range for the <i>drop-count</i> argument is from 1 to 8000000000 bytes. The range for the <i>syslog-level</i> argument is from 1 to 7, and the default level is 4.</p>
Step 9	<p>(Optional) set cos [inner] cos-value</p> <p>Example:</p> <pre>switch(config-pmap-c)# set cos 1</pre>	<p>Specifies the 802.1Q class of service (CoS) value. Use the inner keyword in a Q-in-Q environment. The range is from 0 to 7. The default value is 0.</p>
Step 10	<p>(Optional) set dscp [tunnel] {dscp-value af11 af12 af13 af21 af22 af23 af31 af32 af33 af41 af42 af43 cs1 cs2 cs3 cs4 cs5 cs6 cs7 ef default}</p> <p>Example:</p> <pre>switch(config-pmap-c)# set dscp 10</pre>	<p>Specifies the differentiated services code point value in IPv4 and IPv6 packets. Use the tunnel keyword to set tunnel encapsulation. The range is from 0 to 63. The default value is 0.</p>
Step 11	<p>(Optional) set precedence [tunnel] {prec-value critical flash flash-override immediate internet network priority routine}</p> <p>Example:</p> <pre>switch(config-pmap-c)# set precedence 2</pre>	<p>Specifies the precedence value in IPv4 and IPv6 packets. Use the tunnel keyword to set tunnel encapsulation. The range is from 0 to 7. The default value is 0.</p>
Step 12	<p>exit</p> <p>Example:</p> <pre>switch(config-pmap-c)# exit switch(config-pmap)#</pre>	<p>Exits policy map class configuration mode.</p>

	Command or Action	Purpose
Step 13	exit Example: <pre>switch(config-pmap)# exit switch(config)#</pre>	Exits policy map configuration mode.
Step 14	(Optional) show policy-map type control-plane [expand] [name <i>class-map-name</i>] Example: <pre>switch(config)# show policy-map type control-plane</pre>	Displays the control plane policy map configuration.
Step 15	(Optional) copy running-config startup-config Example: <pre>switch(config)# copy running-config startup-config</pre>	Copies the running configuration to the startup configuration.

Related Topics

[Configuring a Control Plane Class Map](#), on page 22

Configuring the Control Plane Service Policy

You can configure one or more policy maps for the CoPP service policy.

Before you begin

Ensure that you are in the default VDC.

Ensure that you have configured a control plane policy map.

SUMMARY STEPS

1. **configure terminal**
2. **control-plane**
3. **service-policy input** *policy-map-name*
4. **exit**
5. (Optional) **show running-config copp [all]**
6. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
Step 2	control-plane Example:	Enters control plane configuration mode.

	Command or Action	Purpose
	<pre>switch(config)# control-plane switch(config-cp)#</pre>	
Step 3	<p>service-policy input <i>policy-map-name</i></p> <p>Example:</p> <pre>switch(config-cp)# service-policy input PolicyMapA</pre>	<p>Specifies a policy map for the input traffic. Repeat this step if you have more than one policy map.</p> <p>Use the no service-policy input <i>policy-map-name</i> command to remove the policy from the control plane.</p>
Step 4	<p>exit</p> <p>Example:</p> <pre>switch(config-cp)# exit switch(config)#</pre>	Exits control plane configuration mode.
Step 5	<p>(Optional) show running-config copp [all]</p> <p>Example:</p> <pre>switch(config)# show running-config copp</pre>	Displays the CoPP configuration.
Step 6	<p>(Optional) copy running-config startup-config</p> <p>Example:</p> <pre>switch(config)# copy running-config startup-config</pre>	Copies the running configuration to the startup configuration.

Related Topics

[Configuring a Control Plane Policy Map](#), on page 24

Configuring the CoPP Scale Factor Per Line Card

You can configure the CoPP scale factor per line card.

The scale factor configuration is used to scale the policer rate of the applied CoPP policy for a particular line card. The accepted value is from 0.10 to 2.00. You can increase or reduce the policer rate for a particular line card without changing the current CoPP policy. The changes are effective immediately, so you do not need to reapply the CoPP policy.



Note CoPP programming is performed on the forwarding engines of each I/O module. The Cisco Nexus 7000 M Series I/O modules can contain 1 or 2 forwarding engines and the Cisco Nexus7000 F Series modules can contain from 6 to 12 forwarding engines, depending on the module.

If the same CoPP policy profile (strict) that is used for M Series modules is applied on the F Series modules, the traffic that comes to the supervisor from the F Series modules can be many times more than the traffic that comes from the M Series modules and can overwhelm the supervisor. To avoid overwhelming the supervisor, you can configure the dense CoPP profile for F Series modules and certain combinations of F and M Series modules.

Follow these guidelines for configuring the scale factor per I/O module and for applying the appropriate CoPP policy profile, based on the installed I/O modules:

- When a chassis is fully loaded with F Series modules, we recommend that you apply the dense profile without any scale-factor configuration.
- When a chassis is fully loaded with M Series modules, we recommend that you apply the strict profile without any scale-factor configuration.
- When a chassis is loaded with more F series line cards than M series line cards, we recommend that you apply the dense profile and configure a scale-factor value 2 only on the M series line cards.
- When a chassis is loaded with more M series line cards than F series line cards, we recommend that you apply the strict profile and configure a scale-factor value 0.4 only on the F series line cards.

Before you begin

Ensure that you are in the default VDC.

SUMMARY STEPS

1. **configure terminal**
2. **control-plane**
3. **scale-factor** *value* **module** *multiple-module-range*
4. (Optional) **show running-config copp** [**all**]
5. (Optional) **show policy-map interface control-plane** [**class** *class-map* | **module** *slot*]
6. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
Step 2	control-plane Example:	Enters control plane configuration mode.

	Command or Action	Purpose
	<pre>switch(config)# control-plane switch(config-cp)#</pre>	
Step 3	<p>scale-factor <i>value</i> module <i>multiple-module-range</i></p> <p>Example:</p> <pre>switch(config-cp)# scale-factor 1.10 module 1-2</pre>	<p>Configures the policer rate per line card. The allowed scale factor value is from 0.10 to 2.00. When the scale factor value is configured, the policing values are multiplied by the corresponding scale factor value of the module, and it is programmed in the particular module.</p> <p>To revert to the default scale factor value of 1.00, use the no scale-factor <i>value</i> module <i>multiple-module-range</i> command, or explicitly set the default scale factor value to 1.00 using the scale-factor 1 module <i>multiple-module-range</i> command.</p>
Step 4	<p>(Optional) show running-config copp [all]</p> <p>Example:</p> <pre>switch(config-cp)# show running-config copp</pre>	Displays the CoPP configuration in the running configuration.
Step 5	<p>(Optional) show policy-map interface control-plane [class <i>class-map</i> module <i>slot</i>]</p> <p>Example:</p> <pre>switch(config-cp)# show policy-map interface control-plane</pre>	Displays the applied scale factor values when a CoPP policy is applied.
Step 6	<p>(Optional) copy running-config startup-config</p> <p>Example:</p> <pre>switch(config)# copy running-config startup-config</pre>	Copies the running configuration to the startup configuration.

Changing or Reapplying the Default CoPP Policy

You can change to a different default CoPP policy, or you can reapply the same default CoPP policy.



Note In Cisco NX-OS releases prior to 5.2, you must use the setup utility to change or reapply the default CoPP policy. You can access the setup utility using the **setup** command.

SUMMARY STEPS

1. [no] **copp profile** [**strict** | **moderate** | **lenient** | **dense**]
2. (Optional) **show copp status**
3. (Optional) **show running-config copp**

DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>[no] copp profile [strict moderate lenient dense]</code> Example: <code>switch(config)# copp profile moderate</code>	Applies the CoPP best practice policy.
Step 2	(Optional) <code>show copp status</code> Example: <code>switch(config)# show copp status</code>	Displays the CoPP status, including the last configuration operation and its status. This command also enables you to verify that the CoPP best practice policy is attached to the control plane.
Step 3	(Optional) <code>show running-config copp</code> Example: <code>switch(config)# show running-config copp</code>	Displays the CoPP configuration in the running configuration.

Related Topics

[Changing or Reapplying the Default CoPP Policy Using the Setup Utility](#), on page 42

Copying the CoPP Best Practice Policy

The CoPP best practice policy is read-only, beginning with Cisco NX-OS Release 5.2. If you want to modify its configuration, you must copy it.

SUMMARY STEPS

1. `copp copy profile {strict | moderate | lenient | dense} {prefix | suffix} string`
2. (Optional) `show copp status`
3. (Optional) `show running-config copp`

DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>copp copy profile {strict moderate lenient dense} {prefix suffix} string</code> Example: <code>switch# copp copy profile strict prefix abc</code>	Creates a copy of the CoPP best practice policy. CoPP renames all class maps and policy maps with the specified prefix or suffix.
Step 2	(Optional) <code>show copp status</code> Example: <code>switch# show copp status</code>	Displays the CoPP status, including the last configuration operation and its status. This command also enables you to verify that the copied policy is not attached to the control plane.
Step 3	(Optional) <code>show running-config copp</code> Example: <code>switch# show running-config copp</code>	Displays the CoPP configuration in the running configuration, including the copied policy configuration.

Verifying the CoPP Configuration

To display CoPP configuration information, perform one of the following tasks:

Command	Purpose
show policy-map type control-plane [expand] [name <i>policy-map-name</i>]	Displays the control plane policy map with associated class maps and CIR and BC values.
show policy-map interface control-plane [class <i>class-map</i> module <i>slot</i>]	<p>Displays the policy values with associated class maps and drops per policy or class map. It also displays the scale factor values when a CoPP policy is applied. When the scale factor value is the default (1.00), it is not displayed.</p> <p>Note The scale factor changes the CIR, BC, PIR, and BE values internally on each module, but the display shows the configured CIR, BC, PIR, and BE values only. The actual applied value on a module is the scale factor multiplied by the configured value.</p>
show class-map type control-plane [<i>class-map-name</i>]	Displays the control plane class map configuration, including the ACLs that are bound to this class map.

Command	Purpose
show copp diff profile {strict moderate lenient dense} [prior-ver] profile {strict moderate lenient dense}	<p>Displays the difference between two CoPP best practice policies.</p> <p>When you do not include the prior-ver option, this command displays the difference between two currently applied default CoPP best practice policies (such as the currently applied strict and currently applied moderate policies).</p> <p>When you include the prior-ver option, this command displays the difference between a currently applied default CoPP best practice policy and a previously applied default CoPP best practice policy (such as the currently applied strict and the previously applied lenient policies).</p>
show copp profile {strict moderate lenient dense}	<p>Displays the details of the CoPP best practice policy, along with the classes and policer values.</p>
show ip access-lists [acl-name]	<p>Displays the access lists, including the ACLs. If the statistics per-entry command is used, it also displays hit counts for specific entries.</p>
show running-config aclmgr [all]	<p>Displays the user-configured access control lists (ACLs) in the running configuration. The all option displays both the default (CoPP-configured) and user-configured ACLs in the running configuration.</p>
show running-config copp [all]	<p>Displays the CoPP configuration in the running configuration.</p>
show startup-config aclmgr [all]	<p>Displays the user-configured access control lists (ACLs) in the startup configuration. The all option displays both the default (CoPP-configured) and user-configured ACLs in the startup configuration.</p>

For detailed information about the fields in the output from these commands, see the *Cisco Nexus 7000 Series NX-OS Security Command Reference*.

Displaying the CoPP Configuration Status

Before you begin

Ensure that you are in the default VDC.

SUMMARY STEPS

1. switch# **show copp status**

DETAILED STEPS

	Command or Action	Purpose
Step 1	switch# show copp status	Displays the configuration status for the CoPP feature.

Example

This example shows how to display the CoPP configuration status:

```
switch# show copp status
```

Monitoring CoPP

Before you begin

Ensure that you are in the default VDC.

SUMMARY STEPS

1. switch# **show policy-map interface control-plane** {[**module** *module-number* [**inst-all**]] [**class** {*class-map* | **violated**}] | [**class** {*class-map* | **violated**}] [**module** *module-number* [**inst-all**]]}

DETAILED STEPS

	Command or Action	Purpose
Step 1	switch# show policy-map interface control-plane {[module <i>module-number</i> [inst-all]] [class { <i>class-map</i> violated }] [class { <i>class-map</i> violated }] [module <i>module-number</i> [inst-all]]}	Displays packet-level statistics for all classes that are part of the applied CoPP policy. Statistics are specified in terms of OutPackets (packets admitted to the control plane) and DropPackets (packets dropped because of rate limiting).

	Command or Action	Purpose
		<p>Note With Supervisor 3 or F2e Series modules, the output of this command uses Layer 3 packet lengths when displaying the byte count. With M1, M2, or F2 Series modules, the command output uses Layer 2 packet lengths for the byte count.</p>

Example

This example shows how to monitor CoPP:

```
switch# show policy-map interface control-plane
Control Plane
  service-policy input copp-system-p-policy-strict

class-map copp-system-p-class-critical (match-any)
  match access-group name copp-system-p-acl-bgp
  match access-group name copp-system-p-acl-rip
  match access-group name copp-system-p-acl-vpc
  match access-group name copp-system-p-acl-bgp6
  match access-group name copp-system-p-acl-lisp
  match access-group name copp-system-p-acl-ospf
  match access-group name copp-system-p-acl-rip6
  match access-group name copp-system-p-acl-rise
  match access-group name copp-system-p-acl-eigrp
  match access-group name copp-system-p-acl-lisp6
  match access-group name copp-system-p-acl-ospf6
  match access-group name copp-system-p-acl-rise6
  match access-group name copp-system-p-acl-eigrp6
  match access-group name copp-system-p-acl-otv-as
  match access-group name copp-system-p-acl-mac-l2pt
  match access-group name copp-system-p-acl-mpls-ldp
  match access-group name copp-system-p-acl-mpls-rsvp
  match access-group name copp-system-p-acl-mac-l3-isis
  match access-group name copp-system-p-acl-mac-otv-isis
  match access-group name copp-system-p-acl-mac-fabricpath-isis
  match protocol mpls router-alert
  set cos 7
  police cir 36000 kbps bc 250 ms
    conform action: transmit
    violate action: drop
  module 12:
    conformed 0 bytes,
      5-min offered rate 0 bytes/sec
      peak rate 0 bytes/sec
    violated 0 bytes,
      5-min violate rate 0 bytes/sec
      peak rate 0 bytes/sec
  module 14:
    conformed 0 bytes,
      5-min offered rate 0 bytes/sec
      peak rate 0 bytes/sec
    violated 0 bytes,
      5-min violate rate 0 bytes/sec
      peak rate 0 bytes/sec

class-map copp-system-p-class-important (match-any)
  match access-group name copp-system-p-acl-cts
```

```

match access-group name copp-system-p-acl-glbp
match access-group name copp-system-p-acl-hsrp
match access-group name copp-system-p-acl-vrrp
match access-group name copp-system-p-acl-wccp
match access-group name copp-system-p-acl-hsrp6
match access-group name copp-system-p-acl-vrrp6
match access-group name copp-system-p-acl-opflex
match access-group name copp-system-p-acl-mac-lldp
match access-group name copp-system-p-acl-mac-mvrp
match access-group name copp-system-p-acl-mac-flow-control
set cos 6
police cir 1400 kbps bc 1500 ms
  conform action: transmit
  violate action: drop
module 12:
  conformed 0 bytes,
    5-min offered rate 0 bytes/sec
  peak rate 0 bytes/sec
  violated 0 bytes,
    5-min violate rate 0 bytes/sec
  peak rate 0 bytes/sec
module 14:
  conformed 0 bytes,
    5-min offered rate 0 bytes/sec
  peak rate 0 bytes/sec
  violated 0 bytes,
    5-min violate rate 0 bytes/sec
  peak rate 0 bytes/sec
....

```

This example shows the 5-minute moving averages and peaks of the conformed and violated byte counts in the output of the **show policy-map interface control-plane** command. In this example, the 5-minute offered rate is the 5-minute moving average of the conformed bytes, the 5-minute violate rate is the 5-minute moving average of the violated bytes, and the peak rate is the highest value since boot-up or counter reset.

```

class-map copp-system-p-class-multicast-router (match-any)
match access-group name copp-system-p-acl-pim
match access-group name copp-system-p-acl-msdp
match access-group name copp-system-p-acl-pim6
match access-group name copp-system-p-acl-pim-reg
match access-group name copp-system-p-acl-pim6-reg
match access-group name copp-system-p-acl-pim-mdt-join
match protocol mpls exp 6
set cos 6
police cir 2600 kbps bc 1000 ms
  conform action: transmit
  violate action: drop
module 12:
  conformed 0 bytes,
    5-min offered rate 0 bytes/sec
  peak rate 0 bytes/sec
  violated 0 bytes,
    5-min violate rate 0 bytes/sec
  peak rate 0 bytes/sec
module 14:
  conformed 0 bytes,
    5-min offered rate 0 bytes/sec
  peak rate 0 bytes/sec
  violated 0 bytes,
    5-min violate rate 0 bytes/sec
  peak rate 0 bytes/sec

```

This example displays the output of strict profile policy:

```

switch# show copp profile strict
ip access-list copp-system-p-acl-bgp
  permit tcp any gt 1024 any eq bgp
  permit tcp any eq bgp any gt 1024
ipv6 access-list copp-system-p-acl-bgp6
  permit tcp any gt 1024 any eq bgp
  permit tcp any eq bgp any gt 1024
ip access-list copp-system-p-acl-cts
  permit tcp any any eq 64999
  permit tcp any eq 64999 any
ip access-list copp-system-p-acl-dhcp
  permit udp any eq bootpc any
  permit udp any neq bootps any eq bootps
ip access-list copp-system-p-acl-dhcp-relay-response
  permit udp any eq bootps any
  permit udp any any eq bootpc
ipv6 access-list copp-system-p-acl-dhcp6
  permit udp any eq 546 any
  permit udp any neq 547 any eq 547
ipv6 access-list copp-system-p-acl-dhcp6-relay-response
  permit udp any eq 547 any
  permit udp any any eq 546
ip access-list copp-system-p-acl-eigrp
  permit eigrp any any
ipv6 access-list copp-system-p-acl-eigrp6
  permit eigrp any any
ip access-list copp-system-p-acl-ftp
  permit tcp any any eq ftp-data
  permit tcp any any eq ftp
  permit tcp any eq ftp-data any
  permit tcp any eq ftp any
ip access-list copp-system-p-acl-glbp
  permit udp any eq 3222 224.0.0.0/24 eq 3222
ip access-list copp-system-p-acl-hsrp
  permit udp any 224.0.0.2/32 eq 1985
  permit udp any 224.0.0.102/32 eq 1985
ipv6 access-list copp-system-p-acl-hsrp6
  permit udp any ff02::66/128 eq 2029
ip access-list copp-system-p-acl-http-response
  permit tcp any eq 80 any gt 1024
  permit tcp any eq 443 any gt 1024
ipv6 access-list copp-system-p-acl-http6-response
  permit tcp any eq 80 any gt 1024
  permit tcp any eq 443 any gt 1024
ip access-list copp-system-p-acl-icmp
  permit icmp any any echo
  permit icmp any any echo-reply
ipv6 access-list copp-system-p-acl-icmp6
  permit icmp any any echo-request
  permit icmp any any echo-reply
ip access-list copp-system-p-acl-igmp
  permit igmp any 224.0.0.0/3
ip access-list copp-system-p-acl-lisp
  permit udp any any eq 4342
  permit udp any eq 4342 any
ipv6 access-list copp-system-p-acl-lisp6
  permit udp any any eq 4342
  permit udp any eq 4342 any
mac access-list copp-system-p-acl-mac-cdp-udld-vtp
  permit any 0100.0ccc.cccc 0000.0000.0000
mac access-list copp-system-p-acl-mac-cfsoe
  permit any 0180.c200.000e 0000.0000.0000 0x8843

```

```
permit any 0180.c200.000e 0000.0000.0000
mac access-list copp-system-p-acl-mac-dot1x
  permit any 0180.c200.0003 0000.0000.0000 0x888e
mac access-list copp-system-p-acl-mac-ecp-ack
  permit any 0180.c200.0000 0000.0000.0000 0x8940
  permit 0180.c200.0000 0000.0000.0000 any 0x8940
  permit any any 0x8940
```

Monitoring CoPP with SNMP

Beginning with Cisco NX-OS Release 6.2(2), CoPP supports the Cisco class-based QoS MIB (cbQoS MIB). All of the CoPP elements can now be monitored (but not modified) using SNMP. This feature applies only to policies and their subelements (such as classes, match rules, and set actions) that are attached to the control plane. Elements of policies that are not in service on the control plane are not visible through SNMP.

The following cbQoS MIB tables are supported:

- ccbQoSServicePolicy
- cbQoSInterfacePolicy
- cbQoSObjects
- cbQoSPolicyMapCfg
- cbQoSClassMapCfg
- cbQoSMatchStmtCfg
- cbQoSPoliceCfg
- cbQoSSetCfg

More detailed information on cbQoS MIB tables and elements is available at the following urls:

- <http://tools.cisco.com/Support/SNMP/do/BrowseOID.do?local=en&translate=Translate&objectInput=1.3.6.1.4.1.9.9.166>
- http://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus6000/sw/system_management/7x/b_6k_System_Mgmt_Config_7x/b_6k_System_Mgmt_Config_7x_chapter_010110.html

Clearing the CoPP Statistics

Before you begin

Ensure that you are in the default VDC.

SUMMARY STEPS

1. (Optional) switch# **show policy-map interface control-plane** [*class class-map* | **module slot**]
2. switch# **clear copp statistics**

DETAILED STEPS

	Command or Action	Purpose
Step 1	(Optional) switch# show policy-map interface control-plane [class <i>class-map</i> module <i>slot</i>]	Displays the currently applied CoPP policy and per-class statistics.
Step 2	switch# clear copp statistics	Clears the CoPP statistics.

Example

This example shows how to clear the CoPP statistics for your installation:

```
switch# show policy-map interface control-plane
switch# clear copp statistics
```

Configuration Examples for CoPP

This section includes example CoPP configurations.

CoPP Configuration Example

The following example shows how to configure CoPP using IP ACLs and MAC ACLs:

```
configure terminal
ip access-list copp-system-acl-igmp
permit igmp any 10.0.0.0/24

ip access-list copp-system-acl-msdp
permit tcp any any eq 639

mac access-list copp-system-acl-arp
permit any any 0x0806

ip access-list copp-system-acl-tacas
permit udp any any eq 49

ip access-list copp-system-acl-gre
permit 47 any any

ip access-list copp-system-acl-ntp
permit udp any 10.0.1.1/23 eq 123

ip access-list copp-system-acl-icmp
permit icmp any any

class-map type control-plane match-any copp-system-class-critical
match access-group name copp-system-acl-igmp
match access-group name copp-system-acl-msdp

class-map type control-plane match-any copp-system-class-important
match access-group name copp-system-acl-gre

class-map type control-plane match-any copp-system-class-normal
match access-group name copp-system-acl-icmp
```

```

match exception ip icmp redirect
match exception ip icmp unreachable
match exception ip option
match redirect arp-inspect
match redirect dhcp-snoop

policy-map type control-plane copp-system-policy

class copp-system-class-critical
police cir 2000 kbps bc 1500 bytes pir 3000 kbps be 1500 bytes conform
    transmit exceed transmit violate drop

class copp-system-class-important
police cir 1000 kbps bc 1500 bytes pir 1500 kbps be 1500 bytes conform
    transmit exceed transmit violate drop

class copp-system-class-normal
police cir 400 kbps bc 1500 bytes pir 600 kbps be 1500 bytes conform
    transmit exceed transmit violate drop

class class-default
police cir 200 kbps bc 1500 bytes pir 300 kbps be 1500 bytes conform
    transmit exceed transmit violate drop

control-plane
service-policy input copp-system-policy

```

The following example shows how to create the CoPP class and associate an ACL:

```

class-map type control-plane copp-arp-class
match access-group name copp-arp-acl

```

The following example shows how to add the class to the CoPP policy:

```

policy-map type control-plane copp-system-policy
class copp-arp-class
police pps 500

```

Preventing CoPP Overflow by Splitting ICMP Pings and ARP Requests

Some servers use ICMP pings and ARP requests to the default gateway to verify that the active NIC still has access to the aggregation switch. As a result, if the CoPP values are exceeded, CoPP starts dropping traffic for all networks. One malfunctioning server can send out thousands of ICMP pings and ARP requests, causing all servers in one aggregation block to lose their active NIC and start swapping NICs.

If your server is configured as such, you can minimize the CoPP overflow by splitting the ICMP pings and ARP requests based on subnets or groups of subnets. Then if a server malfunctions and overflows CoPP, the supervisor answers the ICMP pings and ARP requests only on some subnetworks.

The last entry in the class map or policy map should identify all of the ICMP pings and ARP requests in the networks that are not specified. If these counters increase, it means that a new network was added that was not specified in the existing ACLs for ICMP and ARP. In this case, you would need to update the ACLs related to ICMP and ARP.



Note Per the default CoPP, ICMP pings fall under `copp-system-p-class-monitoring`, and ARP requests fall under `copp-system-p-class-normal`.

The following example shows how to prevent a CoPP overflow by splitting ICMP and ARP requests.

First, add the new ACLs that identify the networks you want to group together based on the findings of the investigations of the applications:

```
arp access-list copp-arp-1
statistics per-entry
10 permit ip 10.1.1.0 255.255.255.0 mac any
20 permit ip 10.1.2.0 255.255.255.0 mac any
30 permit ip 10.1.3.0 255.255.255.0 mac any
arp access-list copp-arp-2
statistics per-entry
10 permit ip 10.2.1.0 255.255.255.0 mac any
20 permit ip 10.2.2.0 255.255.255.0 mac any
30 permit ip 10.2.3.0 255.255.255.0 mac any
arp access-list copp-arp-3
statistics per-entry
10 permit ip 10.3.1.0 255.255.255.0 mac any
20 permit ip 10.3.2.0 255.255.255.0 mac any
30 permit ip 10.3.3.0 255.255.255.0 mac any
...
arp access-list copp-arp-10
10 permit ip any any mac any

ip access-list copp-icmp-1
statistics per-entry
10 permit icmp 10.2.1.0 255.255.255.0 any
20 permit icmp 10.2.2.0 255.255.255.0 any
30 permit icmp 10.2.3.0 255.255.255.0 any
ip access-list copp-icmp-2
statistics per-entry
10 permit icmp 10.3.1.0 255.255.255.0 any
10 permit icmp 10.3.2.0 255.255.255.0 any
10 permit icmp 10.3.3.0 255.255.255.0 any
ip access-list copp-icmp-3
statistics per-entry
10 permit icmp 10.4.1.0 255.255.255.0 any
10 permit icmp 10.4.2.0 255.255.255.0 any
10 permit icmp 10.4.3.0 255.255.255.0 any
...
ip access-list copp-icmp-10
10 permit icmp any any
```

Add these ACLs to the new class maps for CoPP:

```
class-map type control-plane match-any copp-cm-arp-1
  match access-group name copp-arp-1
class-map type control-plane match-any copp-cm-arp-2
  match access-group name copp-arp-2
class-map type control-plane match-any copp-cm-arp-3
  match access-group name copp-arp-3
...
class-map type control-plane match-any copp-cm-arp-10
  match access-group name copp-arp-10# class-map type control-plane match-any copp-cm-icmp-1

  match access-group name copp-icmp-1
class-map type control-plane match-any copp-cm-icmp-2
  match access-group name copp-icmp-2
class-map type control-plane match-any copp-cm-icmp-3
  match access-group name copp-icmp-3
...
class-map type control-plane match-any copp-cm-icmp-10
  match access-group name copp-icmp-10
```

Modify the CoPP policy map by adding new policies with the above created class maps:

```
policy-map type control-plane copp-system-p-policy
class copp-cm-icmp-1
    police cir X kbps bc X ms conform transmit violate drop
class copp-cm-icmp-2
    police cir X kbps bc X ms conform transmit violate drop
class copp-cm-icmp-3
    police cir X kbps bc X ms conform transmit violate drop
class copp-cm-icmp-4
    police cir X kbps bc X ms conform transmit violate drop
class copp-cm-icmp-10
    police cir X kbps bc X ms conform transmit violate drop
class copp-cm-arp-1
    police cir X kbps bc X ms conform transmit violate drop
class copp-cm-arp-2
    police cir X kbps bc X ms conform transmit violate drop
class copp-cm-arp-3
    police cir X kbps bc X ms conform transmit violate drop
class copp-cm-arp-4
    police cir X kbps bc X ms conform transmit violate drop
class copp-cm-arp-10
    police cir X kbps bc X ms conform transmit violate drop
```

Delete ICMP and ARP from the existing class maps:

```
class-map type control-plane match-any copp-system-p-class-normal
no match protocol arp

class-map type control-plane match-any copp-system-p-class-monitoring
no match access-grp name copp-system-p-acl-icmp
```

Changing or Reapplying the Default CoPP Policy Using the Setup Utility

The following example shows how to change or reapply the default CoPP policy using the setup utility.



Note Beginning with Cisco NX-OS Release 5.2, you can change or reapply the default CoPP policy using the **copp profile** command.

```
switch# setup

---- Basic System Configuration Dialog VDC: 1 ----
```

This setup utility will guide you through the basic configuration of the system. Setup configures only enough connectivity for management of the system.

*Note: setup is mainly used for configuring the system initially, when no configuration is present. So setup always assumes system defaults and not the current system configuration values.

Press Enter at anytime to skip a dialog. Use ctrl-c at anytime

```

to skip the remaining dialogs.

Would you like to enter the basic configuration dialog (yes/no): yes

Do you want to enforce secure password standard (yes/no) [y]: <CR>

  Create another login account (yes/no) [n]: n

  Configure read-only SNMP community string (yes/no) [n]: n

  Configure read-write SNMP community string (yes/no) [n]: n

  Enter the switch name : <CR>

  Enable license grace period? (yes/no) [n]: n

  Continue with Out-of-band (mgmt0) management configuration? (yes/no) [y]: n

  Configure the default gateway? (yes/no) [y]: n

  Configure advanced IP options? (yes/no) [n]: <CR>

  Enable the telnet service? (yes/no) [n]: y

  Enable the ssh service? (yes/no) [y]: <CR>

    Type of ssh key you would like to generate (dsa/rsa) : <CR>

  Configure the ntp server? (yes/no) [n]: n

  Configure default interface layer (L3/L2) [L3]: <CR>

  Configure default switchport interface state (shut/noshut) [shut]: <CR>

  Configure best practices CoPP profile (strict/moderate/lenient/dense/skip) [strict]:
strict

  Configure CMP processor on current sup (slot 6)? (yes/no) [y]: n

  Configure CMP processor on redundant sup (slot 5)? (yes/no) [y]: n

The following configuration will be applied:
password strength-check
no license grace-period
no telnet server enable
no system default switchport
system default switchport shutdown
policy-map type control-plane copp-system-p-policy

Would you like to edit the configuration? (yes/no) [n]: <CR>

Use this configuration and save it? (yes/no) [y]: y

switch#

```

Additional References for CoPP

This section provides additional information related to implementing CoPP.

Related Documents

Related Topic	Document Title
Licensing	<i>Cisco NX-OS Licensing Guide</i>
Command reference	<i>Cisco Nexus 7000 Series NX-OS Security Command Reference</i>

Standards

Standards	Title
RFC 2698	A Two Rate Three Color Marker

Feature History for CoPP

This table lists the release history for this feature.

Table 2: Feature History for CoPP

Feature Name	Releases	Feature Information
CoPP	8.2(6)	Support for uRPF exception CoPP class is introduced.
CoPP	6.2(2)	Updated the output of the show policy-map interface control-plane command to show the 5-minute moving averages and peaks of the conformed and violated byte counts for each policy in each module.
CoPP	6.2(2)	Added VRRP6 ACL support to police VRRP IPv6 traffic. The HSRP ACL is modified to reflect the correct destination addresses of control packets.
CoPP	6.2(2)	Changed the behavior of multicast traffic from being policed at different rates in different classes to being grouped into three classes (multicast-host, multicast-router, and normal) and policed at consistent rates.

Feature Name	Releases	Feature Information
CoPP	6.2(2)	Added the ability to monitor CoPP with SNMP.
CoPP	6.1(1)	Added a new class for FCoE; added the LISP, LISP6, and MAC Layer 3 IS-IS ACLs to the critical class; added the fcoe-fib-miss match exception to the undesirable class; added the MAC Layer 2 tunnel ACL to the Layer 2 unpoliced class, and added the "permit icmp any any 143" rule to the acl-icmp6-msgs ACL.
CoPP	6.0(1)	Added the dense default CoPP policy.
CoPP	6.0(1)	Added the ability to configure the CoPP scale factor per line card.
CoPP	5.2(1)	Added the ability to change or reapply the default CoPP policy without rerunning the setup utility.
CoPP	5.2(1)	Changed the CoPP best practice policy to read-only and added the ability to copy the policy in order to modify it.
CoPP	5.2(1)	Added the show copp profile and show copp diff profile commands to display the details of the CoPP best practice policy and the differences between policies, respectively.
CoPP	5.2(1)	Changed the show running-config aclmgr and show startup-config aclmgr commands to display only the user-configured ACLs (and not also the default CoPP-configured ACLs) in the running and startup configurations.

Feature Name	Releases	Feature Information
CoPP	5.2(1)	Changed the show copp status command to display which flavor of the CoPP best practice policy is attached to the control plane.
CoPP	5.2(1)	Changed the name of the none option for the best practices CoPP profile in the setup utility to skip .
CoPP	5.2(1)	Updated the default class maps with support for MPLS LDP, MPLS OAM, MPLS RSVP, DHCP relay, and OTV-AS.
Control plane policy map	5.1(1)	Added the ability to specify the threshold value for dropped packets and generate a syslog if the drop count exceeds the configured threshold.
CoPP	5.1(1)	Updated the default policies with the 802.1Q class of service (cos) values.
CoPP	5.1(1)	Added support for non-IP traffic classes.
CoPP	5.0(2)	Updated the default policies with support for ACL HSRP6.
CoPP	4.2(3)	Updated the default policies with support for ACL DHCP.
CoPP	4.2(1)	Updated the default policies with support for WCCP and Cisco TrustSec.